106 (Rev. 04/10) Application for a Search Warrant



# UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
[redacted] WILLIS STREET
RICHMOND, VIRGINIA 23224

Case No. 3:19sw 244

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. 2113 | Armed Bank Robbery; Using, Carrying, and Brandishing a Firearm During and In |
| 18 U.S.C. 924(c)(1)(A) | Relation to a Crime of Violence; Aiding and Abetting Bank Robbery; and Forced |
| 18 U.S.C. 2; 18 U.S.C. 2113(e) | Accompaniment during Bank Robbery |

The application is based on these facts:
See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:
Kenneth R. Simon, Jr.

*Applicant's signature*
Joshua Hylton, FBI, TFO
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 8/12/2019

/s/
*Judge's signature*

City and state: Richmond, Virginia

Honorable Roderick C. Young, U.S. Magistrate Judge
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

| IN THE MATTER OF THE SEARCH OF: [redacted] WILLIS STREET RICHMOND, VIRGINIA 23224 | Case No. 3:19SW244 |
|---|---|

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, **Joshua P. Hylton** being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [redacted] **WILLIS STREET, RICHMOND, VA 23224**, hereinafter "**PREMISES**," further described in ATTACHMENT A, for the things described in ATTACHMENT B.

2. Your affiant is a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. I, the undersigned, have over seven years of law enforcement experience stemming from employment as a police officer with the Chesterfield County Police Department. Currently, I am a duly appointed Task Force Officer with the Federal Bureau of Investigation (FBI) and have been so since December 2016. I am assigned to the Richmond FBI's Central Virginia Violent Crimes Task Force where my duties include investigating bank robberies, extraterritorial offenses, armored car robberies, kidnappings, armed carjackings, and theft of government

property. I have investigated numerous criminal violations and have obtained arrest and search warrants that have culminated in the successful prosecutions of their respective offenders. The crimes I investigate are violent in nature and usually involve two or more individuals. I am familiar with the methods violent offenders use to conduct their illegal activities, to include, but not limited to their communication methods, use of additional co-conspirators, and reoccurring method of operation.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information provided is based upon my personal knowledge, or that of other sworn law enforcement officers participating in this investigation.

## RELEVANT STATUTORY PROVISIONS

4. Title 18 U.S.C. § 2113(a) – Bank Robbery

5. Title 18 U.S.C. § 2113(a) and 2 – Aiding and Abetting Bank Robbery

6. 18 U.S.C. § 924(c)(1)(a) – Using, Carrying, and Brandishing a Firearm During and in Relation to a Crime of Violence

7. 18 U.S.C. § 2113(e) – Forced Accompaniment During Bank Robbery

## PROBABLE CAUSE

8. The United States through the FBI's Central Virginia Violent Crimes Task Force (CVVCTF) is conducting a criminal investigation of OKELLO CHATRIE in relation to an armed bank robbery, in violation of Title 18 U.S.C. § 2113.

9. On May 20, 2019, at approximately 4:52 p.m. eastern standard time, the Call Federal Credit Union located at [redacted] Call Federal Drive, Midlothian, VA 23112 was robbed of $195,000 by an armed gunman. At the time, six victims—a mix of customers and employees—were inside the Credit Union. The Credit Union is National Credit Union Administration (NCUA) insured, NCUA Number: 15209.

10. The unknown subject entered the Credit Union, approached victim-teller, J.W., and presented a handwritten note demanding $100,000 and threatening the victim-teller's life: "I've been watching you for sometime now. I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt. I got my boys on the lookout out side. The first cop car they see am going to start hurting everyone in sight, hand over all the cash, I need at least 100k and nobody will get hurt and your family will be set free. Think smartly everyone safety is depending and you and your coworkers action so I hope they don't try nothing stupid."

11. After reading this note, J.W. told the subject that she did not have access to that amount of money. The subject left the demand note in J.W.'s custody and backed away from the counter to produce a silver and black firearm. The subject then directed the victim-teller and the previously unaware customers and employees at gunpoint to move to the center of the lobby and get on the floor. These six victims were then made to walk behind the teller counter to the area where the bank's safe was located.

12. Once near the safe, the subject forced everyone to their knees at gunpoint and demanded that the bank manager open the safe. After the safe was opened, the subject provided the manager with a black and red bookbag in which to place the currency. After acquiring $195,000.00 in United States currency belonging to Call Federal Credit Union, the subject fled the area on foot.

13. After the armed robber left the bank, law enforcement responded. Upon reviewing video surveillance captured inside and outside the bank, law enforcement discovered the following: (1) prior to the robbery, the subject came from behind the southwest corner of an adjacent building, namely Journey Christian Church, at approximately 4:48 p.m.; (2) the subject approached the front entrance of the Credit Union holding a cell phone to the side of his face with his right hand, as if speaking with another party; (3) upon reaching the front entrance of the Credit Union, the subject stood outside for several minutes before entering the bank at approximately 4:52 p.m.; (4) the subject robbed the Credit Union using a silver and black firearm, departing at approximately 4:56 p.m.; and (5) when exiting, the subject ran towards the southwest corner of Journey Christian Church at approximately 4:57 p.m.

14. While forensically processing the scene, law enforcement collected the handwritten demand note and accompanying envelope for latent processing. The items were chemically processed with Ninhydrin, yielding four (4) partial fingerprints of value for identification. The prints were then entered into national law enforcement fingerprint databases. However, no

potential candidates were identified. J.W.'s prints were also collected and compared to the four (4) partial fingerprints. Again, however, no identification was made.

15. On May 20, 2019, law enforcement interviewed the six victims of the armed robbery as well as a witness from Journey Christian Church. The victim-teller described the subject as an approximately 20-30-year-old black male with a height of approximately 5'11'', and a slender build. He/she went on to describe him as having short, braided hair, a scruffy beard, and a foreign accent. Four of the six witnesses recall a strong Jamaican accent. When asked about his clothing, the victim-teller stated that the subject was wearing a gray bucket-style hat with durag underneath, reflective sunglasses, a gray jacket, a reflective construction vest, blue jeans with rips and patches of another blue denim, and black high-top sneakers, resembling Nike Jordans. The firearm brandished during the robbery was silver and black. Other victim accounts indicate the subject carried a small black and red backpack.

16. Based on your Affiant's review of surveillance video from the Call Federal Credit Union, the suspect's attire is visible on the video recording and appears to fit the description set forth in paragraph 15.

17. In addition to speaking with the victim-witnesses, your Affiant also interviewed Journey Christian Church's [redacted] on June 27, 2019. [redacted] recalled his/her encounter with a suspicious individual on May 20, 2019, at approximately 4:30 to 4:40 p.m. [redacted] advised that while exiting through a back door of Journey Church that is located near the southwestern corner of the building, he/she encountered a dark blue Buick sedan parked in the fire

lane approximately four (4) feet from his vehicle. [redacted] further described the Buick as a "newer car, somewhere between 2010-2015 model, with no specific identifiers to note (decals, rims, spoiler, etc)." [redacted] recalled seeing one occupant in the dark blue Buick sedan—a black male wearing reflective sunglasses, reclined in the driver's seat. Similarly, on May 21, 2019, law enforcement interviewed [redacted] who stated that he observed a male in the driver's seat, wearing reflective sunglasses.

18. On June 14, 2019, Your Affiant applied for and obtained a search warrant from a magistrate with Chesterfield County. The search warrant authorized the search of records possessed by Google, Inc., specifically information concerning any Google Account(s) within a certain geographical area (delineated by latitude and longitude) of the Credit Union and surrounding area between 4:20 p.m. and 5:20 p.m. The geographical area focused upon the Credit Union and Journey Christian Church.

19. Based upon Google's return of anonymized information, your Affiant discovered a Google Account that: (1) was near the southwestern corner of Journey Christian Church prior to the robbery at approximately 4:30 to 4:40 p.m.—the time period [redacted] recalled encountering an individual wearing reflective glasses in a blue Buick sedan; (2) was near the southwestern corner of Journey Christian Church prior to the robbery at approximately 4:48 p.m.; (3) was inside the Credit Union during the time of the robbery; and (4) immediately left the area following the robbery, leaving from the southwestern corner of Journey Christian Church. This same Google Account traveled directly from the area of the bank to [redacted] MASON DALE DRIVE, NORTH

CHESTERFIELD, VA 23234. Review of surveillance video from Call Federal Credit Union, as referenced in paragraph 13, corroborates the Google Account's geographical location data during the time of the robbery.

20. Upon your Affiant's request for specific subscriber information for this Google Account, as provided for in the June 14, 2019, search warrant, Google provided the following subscriber information: Name: Jamaican Media; Email: Okellochatrie55@Gmail.com; and Google Account ID: 365520819283.

21. A utilities inquiry of [redacted] MASON DALE DRIVE, NORTH CHESTERFIELD, VA 23234 shows that OKELLO CHATRIE is listed as a subscriber with the following associated telephone number, (804) 475-8298. Based on the similarity between CHATRIE's name and the email associated with the Google Account referenced above, Your Affiant utilized various databases to glean additional information about CHATRIE.

22. These searches revealed that CHATRIE is a 24-year-old black male of Jamaican birth, 6'0" tall, and weighing 180 lbs. In addition, a 2018 photograph shows him with braided hair and an unkempt beard.

23. In light of the physical similarities between CHATRIE and the subject involved in the Credit Union robbery, your Affiant conducted a vehicle inquiry on CHATRIE, which indicated that he owns a blue 2010 Buick Lacrosse with license plate number [redacted]-9548, and vehicle identification number [redacted]1064. A license plate reader (LPR) inquiry indicated OKELLO CHATRIE's dark blue Buick sedan has been observed at [redacted] Mason Dale Drive, North

Chesterfield, VA 23234. The photographs associated with the report revealed, however, that the vehicle was parked at [redacted] MASON DALE DRIVE, NORTH CHESTERFIELD, VA 23234.

24. A law enforcement inquiry of OKELLO CHATRIE revealed that on April 1, 2018, CHATRIE brandished a 10 mm Glock, model G20 pistol at his father and threatened to kill him. In response to the domestic disturbance, Chesterfield County law enforcement officials took CHATRIE and his firearm into custody. Upon your Affiant's review of body worn camera (BWC) associated with CHATRIE's domestic assault, brandishing, and arrest, it is your Affiant's belief that CHATRIE speaks with an accent foreign to the United States, specifically Jamaican and/or "Caribbean Islander." CHATRIE's charges were later nolle prossed and his pistol was never returned to him.

25. As a result, your Affiant conducted a firearm gun log search for CHATRIE. The inquiry indicated that CHATRIE purchased a silver and black 9mm G2C Taurus semiautomatic pistol on April 29, 2019, at Bob Moates Sports Shop, Inc., [redacted] Hull Street Rd, Midlothian, VA 23112. Your Affiant retrieved the Department of Justice Form 4473 filled out by CHATRIE to purchase said firearm.

26. A search of law enforcement databases for CHATRIE indicates no history of pawn shop transactions undertaken by CHATRIE.

27. To further the investigation, your Affiant conducted an inquiry with the Virginia Employment Commission. This search revealed that CHATRIE was employed with Home Depot during the first quarter of 2019. On July 12, 2019, your Affiant visited a Home Depot in Henrico,

VA and learned that CHATRIE was no longer employed with said company. Your Affiant was given a copy of CHATRIE's basic employment data, which yielded the following contact information during his employment with Home Depot:

a. cell phone: (804) 475-8298;

b. email: Okellochatrie55@Gmail.com.

c. Home Address: [redacted] Mason Dale Drive

28. An inquiry of CHATRIE's primary contact number, (804) 475-8298, showed that the service provider is SPRINT. Furthermore, OKELLO CHATRIE is listed as the subscriber. After running CHATRIE's contact number through federal deconfliction databases, it was found that (804) 475-8298 sent/received two (2) text messages and sent/received six (6) phone calls [redacted] during July 2018.

29. On July 17, 2019, your Affiant applied for and obtained a search warrant issued by Magistrate Judge Novak for real time geolocation data. That search warrant was served on SPRINT for CHATRIE's cellular device. On July 17, 2019, SPRINT advised the FBI that the services to (804) 475-8298 were terminated on July 7, 2019.

30. Subsequent to the above, your Affiant sought Sprint toll records for (804) 475-8298. Review of said data shows that 17 minutes prior to the robbery (while parked near the southwestern corner of Journey Christian Church), CHATRIE had a 22-minute phone call with a subject utilizing telephone number [redacted]

31. An inquiry of telephone number [redacted] indicates the subscriber is a resident of [redacted].

32. After further review of CHATRIE's toll records, data shows that 66 minutes after the robbery, CHATRIE had a 20-minute phone call with a subject utilizing telephone number [redacted] An inquiry of said number indicates that [redacted] is the subscriber. [redacted] Law enforcement databases indicate [redacted] resides at [redacted], NORTH CHESTERFIELD, VA 23236.

33. While examining CHATRIE's contact history with [redacted] it was noted that the two devices communicated 157 times between January 1, 2019 and May 25, 2019, with an increase in call duration immediately following the Call Federal Credit Union robbery on May 20, 2019.

a. January 2019: six (6) calls (approximately 18 minutes total)

b. February 2019: 27 calls (approximately 43.5 minutes total)

c. March 2019: 2 calls (approximately three (3) minutes total)

d. April 2019: 9 calls (approximately 19 minutes total)

e. May 01 – May 19, 2019: 72 calls (approximately 140 minutes total)

f. May 20 – May 25, 2019: 41 calls (approximately 237.5 minutes)

34. Due to CHATRIE's association with the [redacted] MASON DALE DRIVE, NORTH CHESTERFIELD, VA 23234 and his travel to the address immediately following the robbery, your Affiant also sought the toll records of CHATRIE's father, [redacted] and sister, [redacted] Review of said data indicates CHATRIE may be utilizing a new and/or additional phone number, (804) 939-3788.

a. In [redacted] records, (804) 939-3788 first appears on May 23, 2019, and is last seen on July 23, 2019. During the referenced time, 12 calls were made between the two devices.

b. In [redacted] records, (804) 939-3788 first appears on May 24, 2019, and is last seen on July 5, 2019. During the referenced time, five (5) calls were made between the two devices.

35. When comparing new phone numbers in [redacted] toll records for after the robbery on May 20, 2019, CHATRIE's new suspected telephone was the only new number in common. In your Affiant's experience, parties responsible for violent crimes often begin using new telephone numbers to conduct their personal or illegal activities shortly following

a criminal act. Furthermore, it is your Affiant's belief that CHATRIE began using (804) 939-3788 to supplement his communication with known associates between the dates of May 23, 2019 and July 7, 2019; whereupon, CHATRIE either used two cellular telephones for communication or swapped SIM cards within the same device to avoid detection by law enforcement.

36. An inquiry of CHATRIE's new suspected number, (804) 939-3788, indicates the service provider is T-Mobile. Furthermore, [redacted] is listed as the subscriber. Law enforcement databases show that [redacted] resides at [redacted], NORTH CHESTERFIELD, VA 23236.

37. This address is further referenced in paragraph 31 and is also associated with [redacted] the individual with whom CHATRIE had a 20-minute call 66 minutes after the robbery. In your Affiant's experience, known associates and/or conspirators of violent offenders, will often aid in the concealment of evidence in the furtherance of criminal activity or in the protection of parties involved. In this instance, it is your Affiant's belief that [redacted] either assisted CHATRIE in acquiring a new account with T-Mobile or allowed him to use a SIM card from a separate device with active service.

38. On July 7, 2018, [redacted] was involved in a domestic dispute between her mother, and mother's boyfriend, [redacted] at [redacted] NORTH CHESTERFIELD, VA 23236. Considering CHATRIE is an associate of both [redacted] and [redacted] and the defendant's increased contact with [redacted] near the time of the robbery, it is your Affiant's belief that both parties have direct knowledge of and/or involvement in the Call Federal Credit Union robbery.

39. On July 18, 2019, an additional LPR check was conducted on CHATRIE's blue 2010 Buick Lacrosse with license plate number [redacted]-9548. The accompanying report indicated that the vehicle had been observed at [redacted] Willis Street, Richmond, Virginia 23224. However, upon response to the area on the date of the inquiry, your Affiant observed the vehicle in question parked in front of [redacted] WILLIS STREET, RICHMOND, VA 23224. After conducting surveillance on this residence for some time, CHATRIE was seen on the front porch with a black female, who was grooming his hair. While law enforcement observed the two parties, CHATRIE approached the blue Buick Lacrosse to retrieve an item out of the back seat.

[redacted]

41. Pursuant to the above surveillance, on July 19, 2019, law enforcement agents applied for and obtained a search warrant from Magistrate Judge David Novak for the placement of a GPS tracking device on CHATRIE's vehicle.

42. Since the GPS device's installment on July 23, 2019, no parties other than CHATRIE have been observed operating the blue Buick Lacrosse registered to him (license plate number [redacted]-9548). Furthermore, review of electronic data associated with the GPS tracking

device on CHATRIE's vehicle shows that on most evening/nights, CHATRIE's Buick Lacrosse is located at the **PREMISES**.

43. During physical surveillance, law enforcement agents captured several still images of CHATRIE's vehicle and presented them to [redacted]—the witness referenced in paragraph 16 of this affidavit—on July 23, 2019. [redacted] noted that the vehicle in the photographs was the same make, model, body shape, color, and year as the vehicle observed behind Journey Christian Church, located at [redacted] Price Club Blvd., Midlothian, VA, prior to the robbery on May 20, 2019.

44. On July 31, 2019, law enforcement met with [redacted] at Journey Christian Church to determine the subject's specific vehicle placement prior to the robbery. During the interview, [redacted] did not specifically recall the gender, race, or whether the defendant was wearing reflective sunglasses.

45. Subsequent to the review of Google Geo data referenced in paragraphs 18 - 20, your Affiant applied for and obtained a search warrant on July 18, 2019, from Magistrate Judge David Novak for the historical Google records associated with account: Okellochatrie55@Gmail.com; and Google Account ID: 365520819283, between the dates of May 1, 2019 and July 15, 2019.

46. Analysis of this location history and activity data associated with CHATRIE's Google account, and technical surveillance data associated with CHATRIE's vehicle revealed the following:

a. during the week prior to the bank robbery (May 13, 2019 to May 19, 2019), location history records indicate that CHATRIE's phone was located near [redacted] MASON DALE DRIVE, NORTH CHESTERFIELD, VA 23234 for 158 hours and near [redacted], NORTH CHESTERFIELD, VA 23236 for approximately seven (7) hours of recorded time;

b. on the day of the bank robbery, May 20, 2019, location history records indicate that CHATRIE's phone was located near the following places:

- 12:00 AM – 10:30 AM [redacted] MASON DALE DRIVE
- 11:01 AM – 11:18 AM Vicinity of Journey Christian Church
- 11:38 AM – 3:35 PM [redacted] MASON DALE DRIVE
- 4:03 PM – 4:51 PM Vicinity of Journey Christian Church
- 4:52 PM – 4:54 PM Call Federal Credit Union
- 4:58 PM – 5:49 PM Genito Road, approaching Courthouse Road
- 5:13 PM – 6:06 PM [redacted] MASON DALE DRIVE
- 6:53 PM – 8:32 PM [redacted] MASON DALE DRIVE
- 8:52 PM – 10:36 PM [redacted]
- 10:56 PM – 11:59 PM [redacted] MASON DALE DRIVE

c. during the week following the bank robbery (May 21, 2019 to May 27, 2019), location history records indicate that CHATRIE's phone was located near [redacted]

MASON DALE DRIVE, NORTH CHESTERFIELD, VA 23234 for 42 hours and near the [redacted], NORTH CHESTERFIELD, VA 23236 for 50 hours of recorded time

d. most recently, during the period of July 23, 2019 to July 28, 2019, technical surveillance was conducted on CHATRIE's vehicle, indicating that CHATRIE was in the vicinity the **PREMISES** for 131 hours of recorded time.

47. Based on the foregoing, it is your Affiant's belief that CHATRIE's lifestyle has significantly changed since the day of the robbery, May 20, 2019. In your Affiant's experience, violent offenders often alter their routines, telephone numbers, places they frequent and/or stay, and who they associate with, following a violent act. Furthermore, such a change normally occurs to avoid law enforcement suspicion and/or detection.

48. Based on law enforcement surveillance of CHATRIE since July 23, 2019, CHATRIE spends most evenings at the **PREMISES**.

49. As a result of the investigation to date, your Affiant has requested law enforcement latent print examiner(s) to conduct direct comparisons of prints recovered from the demand note and accompanying envelope (referenced in paragraph 14), to available fingerprints belonging to CHATRIE and associated parties. At this time, no identifications have been made; therefore, your Affiant believes it is necessary to forensically acquire fingerprints (to include thumbprints), of any individual(s), who are found at [redacted] MASON DALE DRIVE, NORTH CHESTERFIELD, VA 23234, the **PREMISES**, and [redacted], NORTH CHESTERFIELD, VA 23236, and

reasonably believed by law enforcement to be an associate of CHATRIE's. Furthermore, the examination of collected prints from CHATRIE's associates may identify conspirators involved in the robbery.

50. In your Affiant's training and experience, when people act in concert with another to commit a crime, they frequently utilize cellular telephones, computers, tablets, notebook computers, and like devices to communicate with each other through voice calls, text messages, social media accounts, and emails. These COMPUTERS as described in ATTACHMENT B, allow subjects to plan, coordinate, execute, and flee the scene of violent crimes. Furthermore, your Affiant knows that parties involved in violent offenses often use COMPUTERS to gather intelligence information before and after the execution of a robbery or like offense. The examination of such data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device(s) in question.

51. Based on the totality of facts and circumstances referenced herein, your Affiant believes that it is probable CHATRIE is responsible for the armed robbery of the Call Federal Credit Union. As such, your Affiant finds it necessary and prudent to search the **PREMISES** described in ATTACHMENT A for the items described in ATTACHMENT B. The **PREMISES**, being a residence in which Google geolocation data and physical/electronic surveillance show CHATRIE resides (referenced in paragraphs 39, 42, and 46{d}) , likely has evidence and fruits of the crime as described in ATTACHMENT B. In your Affiant's training and experience, parties responsible for violent acts often hide evidence in locations that they reside and in which they have

comfort. As such, the **PREMISES** would be an ideal location for CHATRIE to store items of evidentiary value to the Call Federal Credit Union robbery.

52. Due to the violent nature of the robbery referenced herein, the criminal history or law enforcement contact with CHATRIE's known associates, and likely connection to drug use, manufacturing, sale, and/or narcotics trafficking, your Affiant is requesting authorization for nighttime executions of residential search warrants. It is your Affiant's belief that if granted such, the cover of darkness will aid in the safety of both law enforcement personnel and general public.

**UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES**

53. Through my experience investigating these types of matters, specifically violent crime, I have learned that subjects committing robberies and like offenses are often associated with sophisticated organized crime groups. Investigators commonly see such groups using applications on their mobile devices to send and receive encrypted messages, in both text and voice formats, during the planning and execution of their criminal conduct. Wickr, WhatsApp, Signal, and Telegram are a few examples of mobile applications that allow end-to-end encrypted communication, and as such, are typically beyond the abilities of law enforcement agencies to wiretap. According to the Wickr website, Wickr uses end-to-end encryption, and the "content is encrypted locally on user devices and is only accessible to intended recipients."

54. Several of these secure messaging applications provide an option to set a self-destruct date for messages. Wickr, for example, advertises that messages are ephemeral, and "no conversation lives beyond its useful life – you decide when your content gets automatically deleted

for good." The suspects and their conspirers may choose to place an expiration date on the messages, where at such a time the secure messaging application automatically and irrevocably deletes the conversation from the mobile device. Such deleted conversations cannot be recovered using even the most sophisticated forensic tools available to law enforcement. Wickr also uses an "require authentication" setting that, when enabled, requires the user to enter their Wickr password each time the application is used. If the "require authentication" setting is disabled, Wickr will not prompt for the Wickr password for a short amount of time after the last successful use of the Wickr password, allowing law enforcement a short window in order to access messages send and/or received using the Wickr application. Wickr is not alone in this capability: the other messaging applications operate in a similar manner.

55. Through my experience with previous investigations, your Affiant has known subjects to use multiple mobile devices to communicate with other members of their organization or conspiracy. In some instances, substantial communications discussing criminal acts did not occur via email or text message, but rather through the use of encrypted messaging applications, such as the applications mentioned above. At the time of arrest, investigators have observed messages with expiration dates within the Wickr and other like-applications. However, by the time a forensic examination was conducted, the messages had been erased and were unable to be recovered. In order to preserve these time-sensitive messages, it is essential that investigators be able to access a mobile device immediately.

56. I know from my training and experience, as well as publicly available materials,

that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Examples of such devices providing a fingerprint unlocking capability are several models of Apple's iPhone, as well as several phones, including but not limited to the Samsung Galaxy, which use the Android operating system. Apple iPhones may be fingerprint unlocked using a function called Touch ID, which during setup allows for registering as many as five (5) fingerprints to unlock the device. Samsung's Galaxy S8 and S8+ models may be configured to be unlocked with as many as four (4) fingerprints. In fact, the number of electronic devices providing a fingerprint unlocking capability, including both smart phones and laptops, is growing continually.

57. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based upon the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

58. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

59. In my training and experience, users of electronic devices often enable the above-mentioned biometric features because they are considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. In some instances, biometric features are considered a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

60. As discussed in this affidavit, my training and experience leads me to believe that investigators are likely to find one or more digital devices during the search. The passcode or password that would unlock any such device subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

61. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: 1) more than 48 hours has elapsed since the device was last unlocked; or 2) when the device has not been unlocked using a fingerprint for eight (8) hours *and* the passcode or password has not been entered in the last six (6) days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four (4) hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

62. I have also learned through my training and experience that while the person who is in possession of a device or has the device among his or her belongings at the time the device is found, is likely a user of the device, that person may *not* be the *only* user of that device whose fingerprints are among those that will unlock it. It is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a **PREMISES** without any identifying information on the exterior of the device. Thus, it will likely be necessary

for law enforcement to have the ability to require CHATRIE to attempt to unlock any device recovered from the **PREMISES** using biometric features in the same manner as discussed above.

63. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of these biometric features, the warrant I am applying for would permit law enforcement personnel to: 1) press or swipe the fingers (including thumbs) of CHATRIE to the fingerprint scanner of the device(s) found at the **PREMISES**; 2) hold the device(s) found at the **PREMISES** in front of the face of CHATRIE and activate the facial recognition feature; and/or 3) hold the device(s) found at the **PREMISES** in front of the face of CHATRIE and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. In the event that law enforcement is unable to unlock any cellphone found in the **PREMISES** within the number of attempts permitted by the pertinent operating system, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

64. Due to the foregoing, I request that the Court authorize law enforcement personnel to press the fingers (including thumbs) of individuals found at the **PREMISES** to the fingerprint sensor of any such device found at the **PREMISES** in an attempt to unlock the device and search its contents as authorized by this warrant.

## TECHNICAL TERMS

65. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

66. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage

media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

67. I submit that if a computer or storage medium is found on the **PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Based on my knowledge, training, and experience, when people act in concert with another to commit a crime, they frequently utilize cellular telephones, computers, tablets, notebook computers, and like devices to communicate with each other through voice calls, text messages, social media accounts, and emails. These COMPUTERS as described in ATTACHMENT B, allow subjects to plan,

coordinate, execute, and flee the scene of violent crimes. Furthermore, your Affiant knows that parties involved in violent offenses often use COMPUTERS to gather intelligence information before and after the execution of a robbery or like offense. The examination of such data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device(s) in question. Data from cellular telephone and tablets are often stored via external media hard drives and other backups to COMPUTERS.

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

68. *Forensic Evidence.* As further described in ATTACHMENT B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used

or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use,

who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to plan, coordinate, communicate with conspirators or discuss facts about a robbery or like-crime with known or unknown parties, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

69. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

70. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

71. Because several people share the **PREMISES** as a residence, it is possible that the **PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

## SPECIFICITY OF SEARCH WARRANT RETURN

72. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the **PREMISES** and include a

general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (*e.g.,* "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," *etc.*)

**NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION**

73. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

## CONCLUSION

74. I submit that this affidavit supports probable cause for a warrant to search the **PREMISES** described in ATTACHMENT A and seize the items described in ATTACHMNET B.

Respectfully submitted,

Joshua P. Hylton
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
on August 12, 2019:

/s/
Roderick C. Young
United States Magistrate Judge

**ATTACHMENT A**

*Property to be Searched*

The property to be searched is (1) residence located at [redacted] **WILLIS STREET, RICHMOND, VA 23224** ("**PREMISES**"). The **PREMISES** is a single-family dwelling with blue colored siding and a brick and cinder block base. Furthermore, a driveway is located near the back of the dwelling, which leads to a side door of the **PREMISES** and small blue outbuilding.

**ATTACHMENT B**

*Property to be Seized*

1. United States Currency, to include:

   a. packaging items (money bands and/or bundling material).

2. All records relating to violations of 18 U.S.C § 2113(a) and 2, 18 U.S.C. § 924(c)(1)(a), 18 U.S.C. § 2113(e), and the planning, execution, and concealment of said crimes, to include:

   a. records and information relating to the obtaining, possession, concealment, or transfer of U.S. or foreign currency, including bank records, ATM receipts, money transfer receipts or orders, cashier's checks or receipts, bank drafts, bank checks, prepaid cards, debit cards, payment cards, safe deposit box keys or other similar items;

   b. records and information relating to travel and residence, including lodging, lease agreements, rental vehicles, airline bookings, flights, GPS data from navigation systems, mailing addresses, PO boxes, or similar items;

   c. records and information relating to the conspiracy to commit bank robbery;

   d. records and information relating to using, carrying, and brandishing a firearm during and in relation to a crime of violence; and

   e. records and information relating to the identity or location of additional unknown suspects and/or conspirators.

3. Mobile Telephones that belong to CHATRIE or that may be unlocked using his biometrics.

4. Handwriting samples, to include:

a. notes;

b. legal documents; and

c. journals.

5. Clothing and accessories consistent with items worn by the suspect during the time of robbery, to include:

a. round brimmed hat;

b. reflective sunglasses;

c. long-sleeved shirt;

d. reflective traffic and/or work vest;

e. bookbag;

f. blue jeans; and

g. tennis shoes.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant which can reasonably be tied to CHATRIE and or unlocked by CHATRIE, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER") which can reasonably be tied to CHATRIE and or unlocked by CHATRIE:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and

records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

7. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

8. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

9. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

10. Firearms believed to have been used in the commission of the robbery or otherwise illegally possessed by subjects at the **PREMISES**, to include:

a. receipts of firearm purchase(s) and/or ownership;

b. ammunition and cartridge cases; and

c. firearm boxes.

11. During the execution of the search of the **PREMISES** described in ATTACHMENT A, law enforcement personnel are authorized to: 1) press or swipe the fingers

(including thumbs) of CHATRIE to the fingerprint scanner of the device(s) found at the premises; 2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or 3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

12. Safes and/or other locked containers and doors within the residence or outbuilding(s), having the ability of containing any items referenced in ATTACHMENT B.